EE/CprE/SE 491 Weekly Report 1

Report Coverage: 08/21/2018 - 09/06/2018
Project Title: Security Orchestration Platform
Client: “The Company”
Advisor: Doug Jacobson
Team Members:

- Adam Crosser
- Logan Kinneer
- Daniel Limanowski
- Vijay Uniyal
- Justin RoepschPw
- Paul Chihak

Weekly Summary

As this is the beginning of the semester our primary focus was on conducting research into the techniques, tactics, and procedures used during red team operations as well as identifying areas where we can improve on existing open source and commercial frameworks.

Past Week Accomplishments

Group Accomplishments

- Met with point of contact at “The Company” and discussed ideas and expectations for the project
- Met with team and discussed roles and interests for the project
- Began doing research into technical aspects of the project and identifying areas where we need to learn new tools and frameworks
- Created presentation and elevator pitch for the project to present to the class and to justify why the project is important
- Gained access to SE491 gitlab and code repositories

Individual Accomplishments

- **Adam Crosser:** Learned about a technique called “domain fronting” which allows an attacker essentially “hijack” a legitimate domain and use it for command and control. Began researching windows shellcoding techniques and how it is different from linux. I originally thought writing shellcode for windows would be the same as on linux systems,

but it turns out it is different due to system call numbers being assigned at build time for windows.
- **Daniel Limanowski:** I set up our Slack chat platform and worked with the team to schedule an online, bi-weekly meeting with our client point-of-contact (POC).
- **Vijay Uniyal:** Started basic research on accustoming myself with Python and setting up Django. Also started studying web development as that'll be my primary focus for this project. Slowly starting up React tutorials for the frontend Javascript that'll be needed for the Project.
- **Logan Kinneer:** Researched PowerShell Empire and Cobalt Strike by reading through Cobalt Strike documentation and articles on how to use PowerShell Empire.
- **Paul Chihak:** Looked into possible expansions for our project including adding functionality for automating the testing of malware against different endpoint detection and response systems.
- **Justin Roepsch:** Researched Cobalt Strike features and MetaSploit modules. Brushed up on React, viewed major changes since my last use. Set up my computer to do work on the Gitlab repository.

Pending Issues

We are currently not facing any issues since we have just started on the project our primary focus has been research.

Individual Contributions

Brief summary of individual red team contributions given below.

Name	Individual Contributions	Hours this week	HOURS cumulative
Adam Crosser	Researched covert command control techniques such as domain fronting and began researching how windows shellcode works.	8	8
Daniel Limanowski	Scheduled meeting times, set up Slack, and communicated with "The Company" professionals to	6	6

	understand their client requirements.		
Vijay Uniyal	Basic research in both Django Python(Backend)and React Javascript(FrontEnd)	5	5
Logan Kinneer	Researched both PowerShell Empire and Cobalt Strike	4	4
Paul Chihak	Researched ways to automate deploying malware.	5	5
Justin Roepsch	Researched Cobalt Strike, Metasploit, React	5	5

Plan for the Upcoming Week

- **Group:** While we have met and discussed roles we have not yet formally assigned anyone roles on the team we plan to do this next week.
- **Adam Crosser:** Going to continue to learn about and research the Win32 API and how functions like CreateRemoteThread can be used to inject shellcode into a remote process. Going to research how shellcode works on windows since from what I am reading it is different than on Linux because of the fact that in windows the system call numbers are assigned randomly at build time versus in Linux the system call numbers are static. Because of this in windows in order to call system calls you must call wrapper functions in ntdll.dll in order to make sure there is portability across different builds. This makes it difficult to write shellcode for windows because on linux you can just hard code the system call number whereas on windows you have to use some sort of trick to resolve the address of various DLLs in memory. My plan is to research how this works so I can fully understand this technique. This is important for a red team as there are often cases where you need to inject code into another process using shellcode.
- **Daniel Limanowski:** I plan to get my existing code on our GitLab and meet directly with “The Company” representatives to understand how we can sync code with them so that they can continuously test and deploy my application on their engagements. I will help other team members understand the code I have written thus far and get them up to

speed on developing the application. I plan on beginning to implement new features next week, beginning likely with user authentication.

- **Vijay Uniyal:** I am still quite fresh when it comes to Django/React so I will be further immersing myself in getting comfortable with the software. I also will be acquiring a book about react that I will start studying to help ease myself into the software. Next I will take a look at the already existing code and start understanding what improvements need to be made as well as how the base structure works overall. I plan on helping implement new features, which seems to be User Authentication first.
- **Logan Kinneer:** Meet with the group to discuss what features our offensive security toolkit should have. Obtain a copy of the current webapp and review it's contents. After getting more information about what features the web app has, could have, and should have I can help create and carry out a plan to improve it.
- **Paul Chihak:** I will work with other team members to help them understand the work that has been done so far. Then I will work with the group to help use determine an overarching goal for the project and make sure that everyone is on the same page about what we want to do. I will also continue researching possible paths that our project can take and see which ones are feasible.
- **Justin Roepsch:** I will focus on understanding what we are actually going to do. When the repo gets updated with the current project, I will dive into it to understand what is going on there. I will continue to research different directions we may decide to go with our toolkit.